REMARKS

Reconsideration of the rejections set forth in the Office action dated 6/17/2004 is respectfully requested under the provisions of 37 CFR §1.111(b).

Claims 1-21 were pending.

Claims 22-24 have previously been canceled.

No claims were amended.

Applicant thanks the Examiner for approving the amendments to the specification and for approving the drawings both of which were included with the reply to the office action mailed 12/31/2003.

Applicant hereby notifies the Examiner that US application 09/596,857 entitled *System, Method and Ariticle of Manufacture for Cryptoserver-based Auction*, currently assigned to Examiner Wang, is based on substantually the same specification as the instant application.

I. General Comments regarding the claimed invention

The claimed invention is directed towards determining the price of a **cryptographic service** that identifies the computational burden required to perform the cryptographic service. The cryptographic service is described at page 15, line 19 through page 16, line 4; page 19, lines 13-19; and page 20, lines 17-22.

To summarize, a cryptographic service provider operates a cryptographic server. The cryptographic server provides cryptographic services to clients such that the client can off-load the computational burden related to a cryptographic operation from the client computer to the cryptographic server that provides the service of performing the cryptographic operation. The client pays for the requested cryptographic service (page 21, lines 1-5). One example of such a cryptographic service is that of encrypting data provided by the client (page 19, lines 27-31). Another example is that of performing modular exponentiation (page 16, lines 27-31). Thus, instead of a client computer

performing the cryptographic operation, the client sends a request to a cryptographic server that determines the price of the requested service and performs the requested cryptographic service for the client.

The cryptographic service is thus a service provided by a cryptoserver that off-loads the computational burden due to cryptographic operations from a client computer. The pricing of this service is important as the operator of the client computer needs to be able to determine the cost of using the cryptographic service.

The price charged for the use of the cryptographic service can be based on the computational burden needed to perform the cryptographic service, the privacy level of the cryptographic service, or the speed of performing the cryptographic service. This is described in the instant application with regards to Fig. 7 starting at page 20, line 19 through page 22, line 2 and in particular to page 21 lines 22-30.

The cryptographic service is different from the technology provided by the cited art. In particular, as will be discussed below, nothing in Bhagavath (that simply applies a higher cost for each level of security without ever identifying a computational burden), Iwamura (accounting for an information distribution system), Billstrom (anonymous access to a communication network), and Jakobsson (mix networks), separately or combined teach or suggest a cryptographic service that identifies the computational burden required to perform the cryptographic service.

II. Rejections under 35 USC § 102(e)

Claims 1, 2, 4, 5, 8, 9, 11, 12, 15, 16, 18 and 19 were rejected under 35 USC § 102(e) as being anticipated by Bhagavath et al (6,343,117 B1).

A prima facie case of anticipation is established when the Examiner provides a single reference that teaches or enables each of the claimed elements (arranged as in the claim) expressly or inherently as interpreted by one of ordinary skill in the art.

Applicant respectfully traverses this rejection to the claims as a prima facie case of anticipation has not been established.

Looking first at Bhagavath.

One problem addressed by Bhagavath is that of securely providing VoIP over the Internet (Column 1, lines 42-46). The embodiment addressing this problem is related to Bhagavath Fig. 2. Bhagavath teaches a technology for encrypting VoIP data as it passes through the Internet. The caller is able to use DTMF (touch tones) to enable encryption of the conversation and to specify the level of encryption desired (Column 3, lines 55-59). Once the encryption is selected by the user, Bhagavath informs the user that encryption is enabled and optionally of the associated charges (Column 3, line 64-67) for providing the secure communication at the selected encryption level. The user can change the selected security level if desired (Column 4, lines 2-3).

Turning now to the invention of original claim 1 that is directed to a method for pricing a cryptographic service, comprising:

(a) receiving a request for a cryptographic service;

(b) identifying a computational burden required to perform the cryptographic service, including one or more of a privacy level of the cryptographic service or a speed of performing the cryptographic service; and

(c) determining a price of the cryptographic service based on the at least one of computational burden, privacy level, and speed.

Step (b) includes the limitation of identifying a computation burden for the requested service. As shown in step 720 of figure 7 the computational burden and/or the selected privacy level and/or the selected speed of performance is used to determine the price of the cryptographic service as per element (c) above.

While Bhagavath does teach determining a price for encryption of VoIP data based on the desired privacy level, nothing in Bhagavath teaches step (b) of identifying a computational burden required to perform the cryptographic service. The office action did not provide a citation to Bhagavath supporting that assertion that a computational burden was identified by Bhagavath. Pricing in Bhagavath appears to be value-oriented as is seen by Column 2, lines 28-39 where Bhagavath provides justification for higher

prices but this text does not disclose to one skilled in the art step (b) of the claimed invention.

Thus, original claim1 is not anticipated by Bhagavath. Original claim 8 is directed to a computer program that, when executed by a computer, causes the computer to perform the method of claim 1. Thus, claim 8 is not anticipated for the same reasons as original claim1 is not anticipated.

Original claim 15 is directed to a system that contains logic to perform the method of claim 1. Thus, claim 15 is not anticipated for the same reasons as original claim1 is not anticipated.

Claims 4, 11, and 18 depend on and further limit their respective parent claims and thus are also not anticipated.

Claims 5, 12 and 19 depend on and further limit their respective parent claims and thus are also not anticipated. Applicant respectfully points out that Bhagavath teaches absolutely nothing about Private Information Retrieval which would be understood by one skilled in the art at the time of the invention to mean technology that allows a user to retrieve a record of his/her choice from a database server such that nobody (not even the server) observes the identity of the record. Research on Private Information Retrieval was started around 1995.

II. Rejections under 35 USC §103(a)

Claims 3, 10, and 17 stand rejected under 35 USC §103(a) as being unpatentable over Bhagavath et al (6,343,117 B1) as applied to claims 1, 8, and 15 per the 102(e) rejection and further in view of Iwamura (6,272,535 B1). This rejection is respectfully traversed in view of the following arguments.

A prima facie case of obviousness is established by one or more references that were available to the inventor and that teach a suggestion to combine or modify the reference, the combination or modification of which would appear to be sufficient to have made the claimed invention obvious to one of the ordinary skill in the art.

Applicant respectfully traverses this rejection of claims 1, 3, 8, 10, 15 and 17 as a prima facie case of obviousness was not presented.

With regards to claims 1, 8, and 15, nothing in Bhagavath suggested the need for identifying a computational burden required to perform a cryptographic service. The problem addressed by Bhagavath is that of encrypting data used in VoIP and of charging for that encryption based on the privacy level of the encryption. Nothing in Bhagavath suggests to one skilled in the art a modification to his technology to identify the computation burden required for the cryptographic service as Bhagavath's pricing is simply a function of the specified privacy level and not the computational burden required to provide the privacy level specified. **Thus, claims 1, 8, and 15 are patentable over Bhagavath.**

Turning now to Iwamura.

Iwamura teaches multiple ways to deliver and charge for providing information. The fourth embodiment teaches a user specifying the level of encryption that is to be applied to the information prior to delivery and being charged accordingly. Iwamura does not provide a cryptographic service (as that term is used in the present application) but simply provides a mechanism for providing data that has been protected by a user-selected level of encryption. Nothing in Iwamura separately or combined with Bhagavath teaches a suggestion to one skilled in the art to identify a computational burden. Thus, original **claims 1, 8 and 15** are patentable over Bhagavath in view of Iwamura.

With regards to claims 3, 10 and 17, these claims depend on and further limit their respective parent claims that are patentable. Thus **claims 3, 10 and 17** are patentable.

Claims 6, 13, and 20 stand rejected under 35 USC §103(a) as being unpatentable over Bhagavath et al (6,343,117 B1) as applied to claims 1, 8, and 15 per the 102(e) rejection and further in view of Billstrom (5,729,537). This rejection is respectfully traversed in view of the following arguments.

With regards to claims 1, 8, and 15, nothing in Bhagavath suggested the need for identifying a computational burden required to perform a cryptographic service. The problem addressed by Bhagavath is that of encrypting data used in VoIP and of charging for that encryption based on the privacy level of the encryption. Nothing in Bhagavath suggests to one skilled in the art a modification to his technology to identify the computation burden required for the cryptographic service as Bhagavath's pricing is simply a function of the specified privacy level and not the computational burden required to provide the privacy level specified. Thus, claims 1, 8, and 15 are patentable over Bhagavath.

Billstrom teaches group authentication.

Nothing in Billstrom separately or combined with Bhagavath teaches a suggestion to one skilled in the art to identify a computational burden. Thus, original **claims 1, 8 and 15** are patentable over Bhagavath in view of Billstrom.

With regards to claims 6, 13, and 20 these claims depend on and further limit their respective parent claims that are patentable. Thus **claims 6, 13 and 20** are also patentable.

Claims 7, 14, and 21 stand rejected under 35 USC §103 as being unpatentable over Bhagavath et al (6,343,117 B1) as applied to claims 1, 8, and 15 per the 102(e) rejection and further in view of Jakobsson (6,049,613). This rejection is respectfully traversed in view of the following arguments.

With regards to claims 1, 8, and 15, nothing in Bhagavath suggested the need for identifying a computational burden required to perform a cryptographic service. The problem addressed by Bhagavath is that of encrypting data used in VoIP and of charging for that encryption based on the privacy level of the encryption. Nothing in Bhagavath suggests to one skilled in the art a modification to his technology to identify the computation burden required for the cryptographic service as Bhagavath's pricing is simply a function of the specified privacy level and not the computational burden required to provide the privacy level specified. Thus, claims 1, 8, and 15 are patentable over Bhagavath.

PATENT

Jakobsson teaches mix networks.

Nothing in Jakobsson separately or combined with Bhagavath teaches a suggestion to one skilled in the art to identify a computational burden. Thus, original **claims 1, 8 and 15** are patentable over Bhagavath in view of Jakobsson.

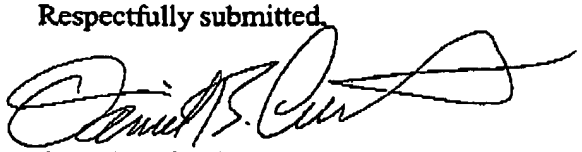
With regards to claims 7, 14, and 21 these claims depend on and further limit their respective parent claims that are patentable. Thus **claims 7, 14 and 21** are also patentable.

Since all rejections, objections and requirements contained in the outstanding official action have been fully answered or traversed and shown to be inapplicable to the present claims, it is respectfully submitted that reconsideration is now in order under the provisions of 37 CFR §1.111(b) and such reconsideration is respectfully requested. Upon reconsideration, it is also respectfully submitted that this application is in condition for allowance and such action is therefore respectfully requested.

No additional fee is believed to be required for this amendment. However, the undersigned Xerox Corporation authorized attorney hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No. 24-0025. This also constitutes a request for any needed extension of time and authorization to charge all fees therefor to Xerox Corporation Deposit Account No. 24-0025.

Should any additional issues remain, or if I can be of any additional assistance, please do not hesitate to contact me at (650) 812-4259.

Respectfully submitted,



Daniel B. Curtis
Attorney for Applicants
Reg. No. 39,159
(650) 812-4259
dbcurtis@parc.com